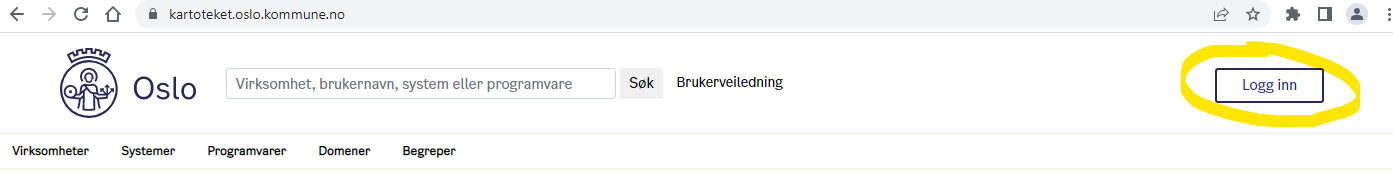
**Om registrering i Kartoteket, v1.5**

**Siden versjon 1 har det blitt opprettet et eget system for behandlingsoversikter! Det er derfor ikke nødvendig å registrere behandlingsprotokoll i kartoteket lenger.**

For å kunne redigere informasjon i Kartoteket må du tildeles rettigheter i PRK-skjemaet «Kartoteket: system- og behandlingsoversikt». Det er fire sentrale roller i skjemaet: En rolle for å registrere behandlinger av personopplysninger, en for registrering av systemer, en for å redigere virksomheter og en for å registrere plattformer. Innlogging skjer med brukernavn, ikke e-postadresse, og det er brukernavnet ditt på felles IKT-plattform som gjelder.

Du finner kartoteket på <https://kartoteket.oslo.kommune.no/>, og du må være tilkoblet VPN for å nå tjenesten per dags dato.

Du må så logge inn med din Oslofelles-ident og passord. Overgang til Azure AD er planlagt, og da logger du på med e-postadresse som brukernavn.



Intensjonen er at de viktigste feltene vises først ved redigering. Det samme prinsippet gjelder visningene, men ulike visninger vil kunne ha ulikt fokus. F.eks. er det andre data som vises i oversikt over systemer din virksomhet drifter, enn i oversikten som viser systemer din virksomhet bruker. Dette arbeidet er pågående og rekkefølgen vil kunne endre seg over tid. Her er dine innspill viktige. Noen felter legges til for å prøve ut nye idéer, mens andre felter fases ut til fordel for mer strukturerte måter å innhente data på. Dette gjøres kontrollert, slik at vi ikke mister noe som er registrert fra før.

Innhold

[Systemer din virksomhet eier eller forvalter 2](#_Toc44437749)

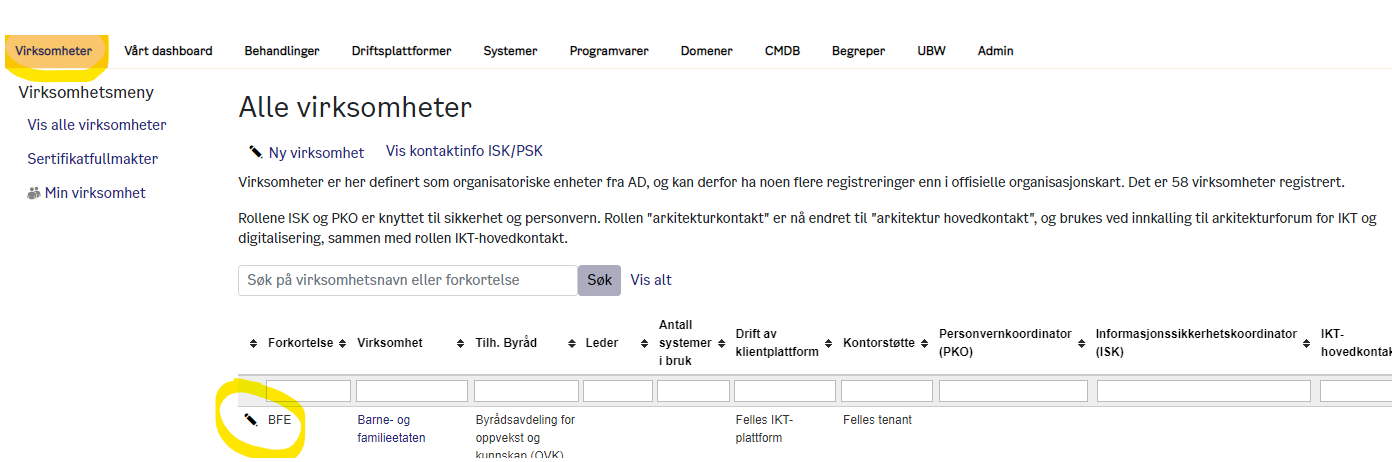
[Systemer (og programvare) din virksomhet bruker 2](#_Toc44437750)

[Virksomhetens behandlingsprotokoll 3](#_Toc44437751)

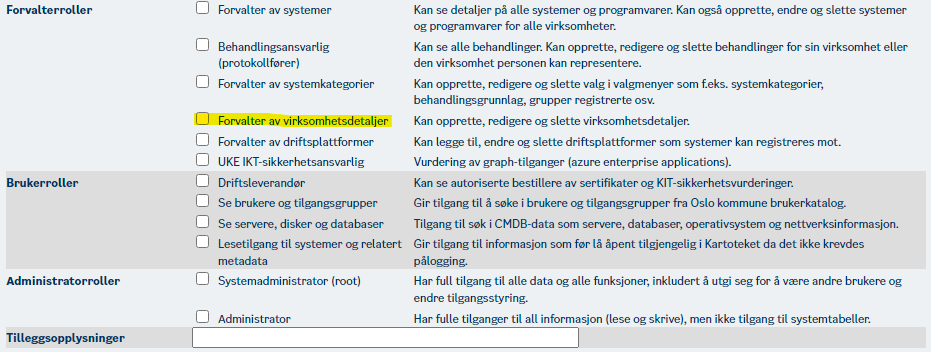
[Personvernsvurderinger og personvernkonsekvensvurderinger (DPIA) 4](#_Toc44437752)

[Annet i Kartoteket 4](#_Toc44437753)

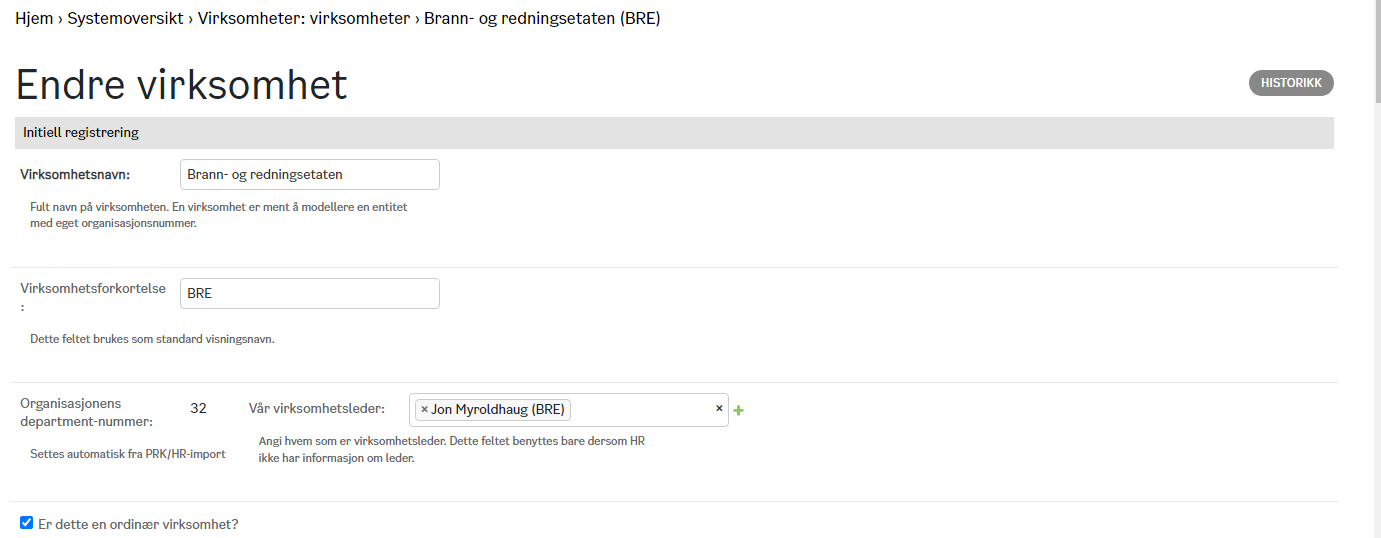
Virksomhetens kontaktpersoner

Du blar deg til «Virksomheter» og finner pennen (merket i gult) ved linjen for din virksomhet.

Pennen er kun synlig om du har rollen «Forvalter av virksomhetsdetaljer» i PRK-skjemaet «Kartoteket: system- og behandlingsoversikt» (fellesskjema).



Når du trykker på pennen tilhørende din virksomhet, får du opp en redigeringsside slik som denne:



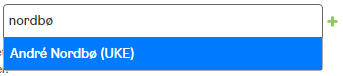
Sjekk at du er inne på riktig virksomhet, og bla deg ned til det feltet du ønsker å endre. Du finner blant annet:

* Vår virksomhetsleder (kun relevant å fylle ut om det mangler fra PRK)
* Vår IKT-hovedkontakt
* Arkitektur hovedkontakter i vår virksomhet
* Personvernkoordinator (PKO)
* Informasjonssikkerhetskoordinator (ISK)
* Administrator for søk i KS Fiks folkeregister portal

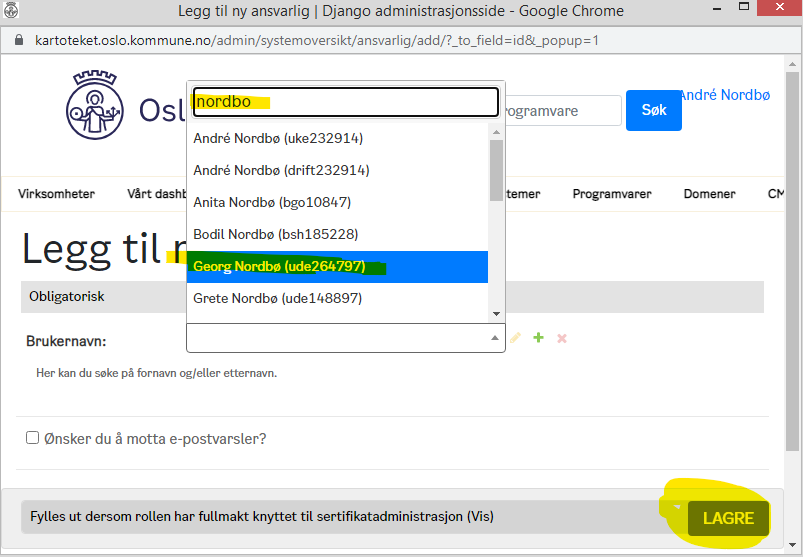
Samt en del andre egenskaper. Alle skal være beskrevet.

Det spesielle med alle steder hvor personer skal oppgis, er at vi har en løsning hvor man velger roller, og ikke personer direkte. Rollene ser ut som personer, men er egentlig «referanser» til personer. Dette er gjort slik for at vi senere skal kunne flytte alt en person er knyttet til over på en annen person når noen slutter eller går ut i permisjon. Dette gjøres via «ansvarlig»-oversiktene. Man velger bare en ansvarlig, endrer personknytningen og lagrer. Alt som før var knyttet til person A er nå over på person B.

For å eksemplifisere ser vi her et forsøk på å søke etter en person. Det er flere i kommunen med samme navn, men kun ett treff vises. Kommer du i en slik situasjon kan du trykke på det grønne + tegnet til høyre for boksen.



Du får da opp et nytt vindu

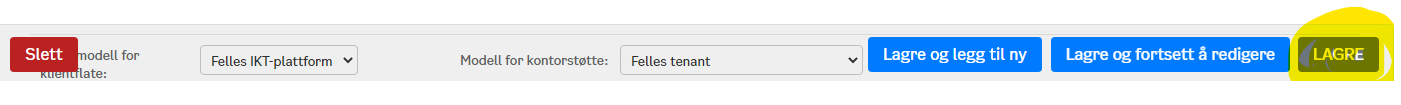


Her kan du søke opp alle personer i kommunen, velge rett person og så lagre. Vinduet forsvinner, og du fortsetter i det opprinnelige skjemaet.

Personen du valgte vil så bli fylt inn automatisk. Du kan så legge til flere personer på samme linje, og du kan slette en person fra valgmenyen ved å trykke på X-en i forkant av navnet.



Når du er ferdig med å legge til nye navn og fjerne eventuelle gamle navn, trykker du lagre på siden.



## Systemer din virksomhet eier eller forvalter

Som grunnregel er det systemforvalter, på vegne av systemeier som registrerer sine systemer i oversikten. Systemforvalter vil i mange tilfeller også registrere felles behandlinger som samsvarer med hvordan systemer er tenkt benyttet. Et hvert system trenger i tillegg til et unikt navn (og eventuelle alias) informasjon om hvordan systemet driftes, hvem som eier og forvalter det, samt ulike former for kategorisering. UKE anbefaler derfor at systemforvaltere har fokus på disse områdene først.

Drift av et system skjer typisk av virksomheten selv, på felles driftsavtale ved UKE, eller av en ekstern leverandør som en tjeneste. Det er opprettet et valg «lokal drift» per virksomhet som per i dag har egen drift. Rollen plattformforvalter kan legge til flere ved behov. Ved drift på felles driftsavtale tar UKE ansvar for å tildele rett driftslokasjon. Ved kjøp av «skytjeneste» brukes valget «Ekstern leverandør (Software as a Service)». Noen ganger registrerer vi systemer som ikke direkte eies/forvaltes av kommunen, men som grenser inn mot våre systemer. Da bruker vi valget «Levert / driftet av en samarbeidspartner». I tillegg til dette er det egne felt for systemleverandør, applikasjonsdriftsleverandør og basisdriftleverandør. For SaaS-tjenester vil det mest riktige være å fylle ut samme på alle tre. Andre ganger har ulike miljø ansvar for de ulike nivåene av drift. Til slutt har vi kategorisering. Systemkategori brukes for å gruppe etter funksjonsområde/bruksområde, systemklassifisering handler om hvor utbredt systemet er. Bare din virksomhet opp til fellessystem der hele kommunen bruker samme system. Vi har også det som kalles systemtype / menneskelig grensesnitt som brukes for å angi brukergrensesnittet til sluttbrukere, samt angi om det er et støttesystem eller f.eks. en integrasjonskomponent. Driftsverktøy angis helst som «infrastrukturkomponent» og får da et 🔧symbol.

Det er mange andre felter du kan registrere. Informasjonsklassifisering, tilgangsstyring, dato og link til systemets risikovurdering, og felter for å angi avhengigheter til andre systemer. De fleste av disse skal være beskrevet.

Virksomhetens kontaktpersoner

## Systemer (og programvare) din virksomhet bruker

Ofte har systemforvalter god oversikt over hvilke virksomheter som bruker deres systemer, men tanken bak Kartoteket er at lokal virksomhet skal kunne gjøre noen ekstra vurdering, samt kunne oppgi lokale kontaktpersoner. I tillegg kan virksomhet velge å abonnere på fellesbehandlinger i stedet for å registrere sine egne (ofte duplikate).



Questback er her valgt ut som eksempel fordi det illustrerer litt av utfordringen, men også fordelen ved bruk av Kartoteket. Questback er levert som en tjeneste av et selskap over Internett. Ingen i Oslo kommune eier eller forvalter Questback på overordnet nivå, men virksomheten kan likevel legge til lokal forvalter (kontaktperson), samt gjøre vurderinger av egnethet og hvor viktig systemet er for deres oppdragsløsning. Dersom din virksomhet benytter et system/tjeneste utom det som er registrert, kan du opprette et nytt og starte å registrere bruken av det. UKE har brukt informasjon innhentet tidligere til å forhåndsutfylte oversikten for din virksomhet, men det kan selvsagt hende at noe har gått ut på dato, eller at noe mangler. Her har vi et felles sted å holde oversikt.

For programvare fungerer det tilsvarende som for systemer, men merk at programvare er noe som installeres lokalt på en datamaskin / klient. Det er derfor langt færre felter som kan fylles ut for programvare. Programvare er ofte en del av et større system, og man kan fra system angi programvare systemer er avhengig av for å virke. Klassisk eksempel er Word, som typisk kreves i spesifikke versjoner av sak- og arkivsystemer.

System- og programvarebruk kan slettes, og da blir den bruken borte. Systemer sletter vi ikke. De setter vi til «ikke i bruk».

## Virksomhetens behandlingsprotokoll

Fra det opprinnelige formålet med Kartoteket var det nettopp å se behandlingen (av personopplysninger) i sammenheng med oversikten over systemene. Kartoteket har i stor grad siden vært drevet av behov relatert til informasjonssikkerhet, it-sikkerhet, personvern og internkontroll.

Registrering av behandling er et omdiskutert tema i kommunen. Kravene i loven er omfattende, men vi har nå lagt oss på et minimumsnivå etter mal fra Datatilsynet. Det er likevel mange spørsmål som bør besvares, og det jobbes med å finne gode strukturer for registrering av svarene på disse.

Helt overordnet må en behandling inneholde svar på hvem de registrerte er (grupper) og hva slags opplysninger det er snakk om. De aller fleste behandlinger skjer i datasystemer, så det vil være helt naturlig at minst ét system er oppgitt. Samtidig ser vi av erfaring at det er forvaltningsmessige argumenter for å holde antall systemer i en behandling til et absolutt minimum. Når du registrerer en behandling mot et system, dukker denne behandlingen opp på detaljsidene til alle systemene du oppgir, tilsvarende som at all bruk av systemet vises der.

Datatilsynet mener også at slettefrister, formål med behandlingen og eventuell utlevering av opplysningene til 3.parter er så viktig at enhver behandling må omtale disse forhold.

For vår egen del trenger vi også å vite hvem som er hovedansvarlig for å vedlikeholde denne linjen i protokollen. Juridisk er virksomhetsleder ansvarlig for behandlingen i sin virksomhet, men i praksis må virksomhetsleder delegere registreringsansvaret. Derfor kobler vi hver behandling til en «ansvarlig» som peker på en konkret person. Vi slår så opp personens seksjon via PRK, slik at du lett kan filtrere ut f.eks. alle som jobber i din seksjon eller avdeling.

Hovedprinsippet er at det holder å ha en behandling registrert én gang innad virksomhetens protokoll. Dersom HR har registrert prosessen knyttet til ansettelser, trenger ikke alle andre legge inn sin egen. Men alle seksjoner/grupper må systematisk gå igjennom protokollen for å identifisere om de har behandling som ikke er nevnt. Videre må ledelsen beslutte hvor eierskapet til denne nye behandlingen skal ligge. Fra UKE sin erfaring ser vi at det er hensiktsmessig at systemforvaltere (tjenesteledere) sørger for at behandlingen knyttet til sine system er registrert, og at denne forvalterrollen er et naturlig sted å forankre dette ansvaret. Typiske unntak her er da skytjenester som f.eks. Questback nevnt før, der ingen eier/forvalter systemet sentralt. Men kan likevel sørge for at behandlingen tar inn over seg alt systemet brukes til, sekundært opprette en ny behandling. Det er også mulig å notere ned hvem som bruker systemet lokalt under virksomhetens «systembruk» av systemet i fritekstfelt der.

Behandlinger systemforvalter markerer som «fellesbehandling» får 🤝 symbolet. Disse behandlingene dukker opp i din virksomhets protokoll dersom dere for denne systembruken har krysset av for «abonner på felles behandlinger i systemet» under «vår bruk av systemer». Dette er valgfritt, og dere kan selvsagt registrer egne enten ved siden av eller i stedet for.

## ~~Personvernsvurderinger og personvernkonsekvensvurderinger (DPIA)~~

~~Det skal gjøres personvernsvurderinger knyttet opp til ivaretakelse av den registrertes rettigheter for de behandlinger vi gjør. Mange av svarene på disse spørsmålene kan registreres som en del av de utvidede feltene per behandling. Det er ikke endelig besluttet en felles metode her, og du vil finne at det også er opprettet egne word-maler for dette.~~

~~Personvernkonsekvensvurderinger, eller DPIA som vurderingene forkortes til, gjøres i situasjoner med høy risiko forbundet med behandlingen. For eksempel grunnet omfattende behandling av spesielle kategorier personopplysninger (helseopplysninger med mer). Det er derfor laget en sjekkliste per behandling i Kartoteket hvor du kan krysse av for de ulike faktorene som til sammen avgjør om DPIA må utføres. Ut over dette er det kun lagt opp til at du kan legge til en URL til der DPIA ligger. Det var et tidlig forsøk på å lage en mal for DPIA i Kartoteket, men dette er nå deaktivert inntil vi eventuelt finner kapasitet til å ta det opp igjen.~~

## Annet i Kartoteket

PRK mottar noe data fra Active Directory og PRK. Mesteparten av denne funksjonaliteten ligger under fanen CMDB. Her kan du søke opp detaljer knyttet til serverdrift, nettverk, PRK-valg og tilgangsgrupper dersom du har nødvendige tilganger. Som hovedregel skal systemforvaltere og behandlingsansvarlige ha tilgang. Vi synkroniserer også data fra felles driftsleverandør regelmessig, noe som lar oss koble systemer til de serverne og databasene som ligger bak.

Det er en modul for domener (URL-er) som er knyttet til systemer der denne er knyttet til registrering av sikkerhetstester som skjer på systemet. Det er derfor fint om du oppgir URL-er til systemer som er web-baserte.

Det er en liten modul for definisjoner, men den er mest eksperimentell. Det er uklart om den vil vedvare.

Du vil finne ulike paneler som grafer opp datakvalitet og f.eks. prosentvis gjennomføring av risikovurderinger. Disse panelene får verdi dersom din virksomhet aktivt fyller ut nødvendige felter på behandlinger og på systemer.

Det er en modul for avtaler. Man kan knytte avtaler til systemer og til plattformer. Avtaler er igjen koblet til leverandører, som igjen er koblet til både behandlinger og systemer. Det er på denne måten mulig å få ut oversikter over hvilke systemer en gitt leverandør har ansvar for, samt hvilke behandlinger de er databehandler for.

Det er mulig å hente ut data fra kartoteket til excel både via nedlasting av excel-rapporter, samt ved tilkobling via API. Sistnevnte er under utprøving. De samme API-ene prøves også ut i Confluence der vi har plugins for enkel pivott og generering av grafer. Dersom du ønsker å gjøre en analyser som ikke understøttes av visinger som allerede er tilrettelagt, kan du få dataene via et API på et valgfritt format. Behov som går igjen kan vi legge opp egne pivottabeller for.